AFRL-RH-WP-TR-2013-0131

The Construct of State-Level Suspicion: A Model and Research Agenda for Automated and Information Technology (IT) Contexts

Dr. Philip Bobko
Departments of Management and Psychology
Gettysburg College

Lt. Col. Alex Barelka, PhD., PMP
Human Effectiveness Directorate
711th Human Performance Wing
Wright-Patterson AFB, OH 45433

Dr. Leanne Hirshfield
SI Newhouse School of Public Communication
Syracuse University

AUGUST 2013

Interim Report for August 2011 – August 2013

AIR FORCE RESEARCH LABORATORY
711TH HUMAN PERFORMANCE WING
HUMAN EFFECTIVENESS DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

Qualified requestors may obtain copies of this report from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RH-WP-TR-2013-0131 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//signature//	//signature//
Alexander Nelson	Louise Carter, Ph.D.
Work Unit Manager	Chief, Human-Centered ISR Division
Human Trust and Interaction Branch	Human Effectiveness Directorate
	711th Human Performance Wing
	Air Force Research Laboratory

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-AUG-2013	Interim	08/2011 – 08/2013

4. TITLE AND SUBTITLE

The Construct of State-Level Suspicion: A Model and Research Agenda for Automated and Information Technology (IT) Contexts

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. Phillip Bobko, Lt Col Alex Barelka, PhD, PMP, Dr. Leanne Hirshfield

5d. PROJECT NUMBER
H0AL

5e. TASK NUMBER

5f. WORK UNIT NUMBER
H0AL (2313HX07)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

Human Trust and Interaction Branch
Human-Centered ISR Division
7llth Human Performance Wing
Human Effectiveness Directorate
Wright-Patterson AFB, OH 45433

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Materiel Command
Air Force Research Laboratory
711th Human Performance Wing
Human Effectiveness Directorate
Human-Centered ISR Division
Human Trust and Interaction Branch
Wright-Patterson AFB OH 45433

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S):

AFRL-RH-TR-WP-2013-0131

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A. Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
88ABW-2014-0406, Cleared 07 February 2014

14. ABSTRACT

The study of suspicion, including its correlates, antecedents, and consequences, is important. We hope that the social sciences will benefit from our integrated definition and model of state suspicion. The research propositions regarding suspicion in IT contexts should motivate substantial research in human factors and related fields.

15. SUBJECT TERMS
Cognitive Activity (CA); Electrodermal Activity (EA); Error-Related Negativity (ERN)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
U	U	U	SAR	35	Lt Col Alex Barelka, Ph.D., PMP

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. 239.18

THIS PAGE INTENTIONALLY LEFT BLANK.

TABLE OF CONTENTS

Section **List**

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

This material is based upon work supported by the Air Force Office of Scientific Research (AFOSR). Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the AFOSR.

We thank the action editor, Heather Odle-Dusseau, and two reviewers for helpful comments on an earlier draft of this manuscript.

PRECIS

An integrative definition and model of state suspicion is developed by reviewing multiple social science disciplines. Research propositions within information technology (IT) contexts are derived.

1.0 SUMMARY

1.1 Objective

Review and integrate available research about the construct of state - level suspicion as it appears in social science literatures. Apply the resulting findings to Information Technology (IT) contexts.

1.2 Background

Although the human factors literature is replete with articles about trust (and distrust) in automation, there is little on the related, but distinct, construct of "suspicion" (either in automated or IT contexts). The construct of suspicion – its precise definition, theoretical correlates, and role in such applications - deserves further study.

1.3 Method

Literatures that consider suspicion are reviewed and integrated. Literatures include communication, psychology, human factors, management, marketing, information technology, and brain/neurology. We first develop a generic model of state- level suspicion. Research propositions are then derived within IT contexts.

1.4 Results

Fundamental components of suspicion include (i) uncertainty, (ii) increased cognitive processing (e.g., generation of alternative explanations for perceived discrepancies), and (iii) perceptions of (mal)intent. State suspicion is defined as the simultaneous occurrence of these three components. Our analysis also suggests that trust inhibits suspicion while distrust can be a catalyst of state-level suspicion. Based on a three-stage model of state-level suspicion, associated research propositions and questions are developed. These propositions and questions are intended to help guide future work on the measurement of suspicion (self-report and neurological), as well as the role of the construct of suspicion in models of decision-making and detection of deception.

1.5 Conclusion

The study of suspicion, including its correlates, antecedents, and consequences, is important. We hope that the social sciences will benefit from our integrated definition and model of state suspicion. The research propositions regarding suspicion in IT contexts should motivate substantial research in human factors and related fields.

2.0 THE CONSTRUCT OF STATE-LEVEL SUSPICION: A MODEL AND RESEARCH AGENDA FOR AUTOMATED AND INFORMATION TECHNOLOGY (IT) CONTEXTS

Suspicion is an important, yet relatively uninvestigated, topic in the social sciences, particularly in technology-oriented contexts. For example, suppose a drone operator is monitoring a computer screen which provides a visual representation of what is being seen while the drone is flying in a remote region of the world. If the information gets unusually blurry, does the operator become suspicious and wonder if the satellite transmission is being affected by solar flares or if the transmission is being tracked by the enemy? Further, assuming the transmission is indeed being tracked (and possibly even purposively distorted), what cues might lead the operator to suspect the attacker has, in turn, become suspicious that others are aware of his covert activities?

Or, imagine an individual who is monitoring electronic transmissions of another computer operator. If the first individual sees an anomaly, does that cause him/her to be suspicious? At what level of perceived malintent do such "triggers" occur? And, what information might lead the first operator to "suspect" that the second operator knows he or she is being monitored? When "suspicion" occurs, what is the psychological state of that first operator? What emotional and cognitive responses are associated with the state of suspicion?

Or, imagine an analyst (financial, military, etc.) who, during a work-related task, encounters an untrustworthy website that asks for personal login information. At what point does s/he become suspicious and/or follow any predefined organizational protocol developed for these malicious situations?

In this review and analysis, we first consider the general construct of suspicion – a construct that, although important, is associated with scant academic research. Borrowing from the trust in automation (and related) literature, we then develop a heuristic model of state-level suspicion in technologically enhanced environments. A framework of relevant factors, research propositions, research questions, and future needs are noted.

3.0 TOWARDS A LITERATURE-BASED DEFINITION OF THE CONSTRUCT OF STATE-LEVEL SUSPICION

3.1 The Social Science Literature on Suspicion

We reviewed several social science literatures for published work that provided definitions of the concept of "suspicion." Literatures included psychology (personality and social psychology subfields), human factors, management, information science, marketing, information technology, and political science (including conflict resolution). We found minimal literature on suspicion. Some of the definitions were about state suspicion (e.g., Fein, 1996; Lyons et al., 2011), some were about more generalized dispositional suspicion (e.g., Buss & Durkee, 1957, or Levine & McCornack, 1991 who had both types), and some articles did not make this distinction. Although we borrow conceptual issues from all of this work, we focus attention on state suspicion, because our resulting model is about the transient state (cf. Bond & Lee, 2005) induced by IT interactions.

The minimal work (often in social psychology) was only sometimes useful. For example, some articles would discuss suspicion as a central variable in their study without defining it (e.g., Ferrin & Dirks, 2003, in management; Hoffman, 2007, in political science; Vonk, 1998 in social psychology; Yoon, Guran-Canli, & Schwartz, 2006, in marketing). If definitions were provided, they were sometimes of questionable use (e.g., Deutsch, 1958, or, in conflict management, Buss & Perry, 1992).[1]

However, some articles provided more guidance regarding components of the suspicion construct, and they are summarized in Table 1. They led to some convergences in our analysis (see the common attributes of uncertainty, malintent, and cognitive activity earmarked in Table 1), although we note that there was no single, consistent conceptual definition of the construct of suspicion in the prior literature (as previously noted by Levine & McCornack, 1991). We summarize this literature, and the entries in Table 1, by discussing the three common components of suspicion that lead to our integrative definition of state suspicion.

[1] Deutsch is an oft-cited early researcher in this domain. His definition of suspicion is "an individual may be said to be suspicious of the occurrence of an event if the disconfirmation of
the expectation of the event's occurrence is preferred to its confirmation and if the expectation of its occurrence leads to behavior which is intended to reduce its negative motivational consequences" (p. 267).

Table 1: Definitions of Suspicion from Social Science Literatures

Social Psychology
Hilton, Fein, and Miller (1993) define suspicion as having two components of "questioning motives" and being in a state of "suspended judgment" (p. 502). Suspicious perceivers "suspend their judgments until they are able to determine" which alternative is accurate (p. 504). It is also noted that suspicion increases cognitive load. **Uncertainty (Un), Cognitive Activity (CA)**
Fein (1996) defines suspicion as "a dynamic state in which the individual actively entertains multiple, plausibly rival hypotheses about the motive or genuineness of a person's behavior" (Fein, 1996, p. 1165). The author also suggests that suspicion additionally implies that the "other" person (i.e., the actor) is hiding something or discrediting the meaning of behavior. **Un, CA, Mal-Intent (MI**)
Sinaceur (2010) adopts Fein's definition of suspicion in dyadic, negotiation contexts (i.e., consideration of plausible, rival hypotheses about another's motives). Notes that suspicion is more than uncertainty because of the additional cognitions about underlying motives, although the motives can be both positive and negative. **Un, *CA*.**
Echebarria-Echabe (2010) defines suspicion as "the preventive attitude of receptors towards a message because they think that it contains biased or hidden interests and involves some attempt at manipulation" (p. 148). **Un, MI**
M**arketing (and Consumer Psychology**)
Campbell and Kirmani (2000) adopt Fein's (1996) definition. **Un, CA, MI**
DeCarlo (2005) defines suspicion (of motives) as a "questioning" (p. 239) of motives that underlie another's behavior. The role of cognitive arousal is also noted. **Un, CA**
Consulting Psychology
Buss and Durkee (1957) define suspicion as "… projection of hostility on to others. This varies from merely being distrustful and wary of people to beliefs that others are being derogatory or are planning harm." In follow-up work (Buss & Perry, 1992), "suspicion" and "resentment" items loaded on the same factor. **MI**
Management
Grant and Hofmann (2011) define suspicion as "questioning the motives or the sincerity of behavior" (ftnte. 2). **Un, MI**
Communication
Buller and Burgoon (1996) define suspicion as "a belief, held without sufficient evidence or proof to warrant certainty, that a person's speech or actions may be duplicitous." (p. 205) **Un, MI.**

Table 1: Definitions of Suspicion from Social Science Literatures (Continued)

Levine and McCornack (1991) define trait suspicion as "a predisposition toward believing that the messages produced by others are deceptive"; state suspicion is "a belief that communication within a specific setting and at a particular time may be deceptive" (p. 328). They also note that suspicion invokes active information processing. ***Un, CA, MI.***
Human Factors
Lyons et al. (2011) define suspicion as "the degree of uncertainty one has when interacting with a particular stimulus," and they note that suspicion is associated with tension and cognitive processing. **Un, CA**
Olson (2009) defines suspicion as "user perceptions that the direction, duration, and intensity of an IT systems unexpected behavior will negatively impact their task" [sic]. **Un, MI**

3.2 The Characteristic of Uncertainty

The factor of "uncertainty" appears as a key facet of several definitions of suspicion. In social psychology, Hilton, Fein, and Miller's (1993) review of the role of suspicion in making inferences suggests that suspicious individuals "*suspend their judgments* [italics added for emphasis] until they are able to determine" which alternative is accurate (p. 504). A similar follow-up definition by Fein (1996) was also adopted by Sinacuer (2010) in his studies on suspicion in two-person negotiation scenarios, as well as by Campbell and Kirmani (2000) in their marketing and consumer behavior studies. This suspension of judgment is consistent with the presence of uncertainty. If individuals were more certain (i.e., below some threshold of uncertainty) they might be more prone to making decisions instead of waiting. Also in social psychology, Echebarria-Echabe (2010) studied students' suspicions when processing persuasive arguments; his definition included an implied uncertainty by students (as well as a concern about motives and intent).

In marketing, DeCarlo (2005) studied students' suspicion of salespersons, which was defined as a "questioning" (p. 239) of the salesperson's motives; hence uncertainty is again implied. In management, Grant and Hofmann (2011) studied the reception of an ideological message in organizations as a function of the characteristics of the message sender. They hypothesized receiver suspicion as a mediating, explanatory variable for their findings, and they defined suspicion as "questioning the motives or the sincerity of behavior" (p. 175). A similar definition appears in the communication literature. For example, Buller and Burgoon (1996) define suspicion as "a belief, held without sufficient evidence or proof to warrant certainty, that a person's speech or actions may be duplicitous" (p. 205). Finally, in human factors, Lyons et al. (2011) define suspicion as "the degree of uncertainty one has when interacting with a particular stimulus" (p. 220) which, in their study, was a computer system that included an automated tool.

Thus, uncertainty is likely an important component in the definition of suspicion. We underscore the "an" because this factor does not, by itself, define suspicion. For example, one can be uncertain about how to operate a software application (due to inexperience), yet not necessarily be suspicious about it.

3.3 The Characteristic of MI

In the literature-based definitions of suspicion, attributions about the intent of an external agent emerged as another important component. For example, in social psychology, Fein (1996) mentions an attribution about the "genuineness" of a person's behavior. He also notes that suspicion implies that the "other" person is hiding something or discrediting the meaning of behavior. Or, in Echebarria-Echabe's (2010) study of persuasive arguments, suspicion is defined as "the preventive attitude of receptors towards a message because they think that it contains biased or hidden interests and involves some attempt at manipulation" (p. 148). In management, Grant and Hofman (2011) use the phrase "questioning the motives"; in communication, Buller and Burgoon (1996) mention that "a person's speech or actions may be duplicitous."

Also, we incorporate "mal" in the notion of "intent" – thereby giving suspicion a negative cast - because almost every article about suspicion assumed the potential for harm and negative outcomes, particularly in cyber contexts. However, suspicion is more general, in that it can also have a positive cast (e.g., "I suspect my family is planning a surprise birthday party for me").[2]

3.4 The Characteristic of Cognitive Activation

Several literatures suggest another important component of suspicion; i.e., a substantial increase in cognitive load when in a state of suspicion (see Bond, 2012 or Patterson, 2009, for some markers of cognitive load, such as inhibition, loss of working memory, reduced processing speed, reduced sensory functioning, excess body movement, or decreased eye blinking). For example, Fein's (1996) social psychological review and definition of suspicion included the cognitive generation/consideration of multiple plausible, rival hypotheses for observed behavior. He notes research support for such increased cognitive activity (p. 1167). In adopting Fein's definition in negotiation contexts, Sinaceur (2010) also notes associated increases in cognition.

In the communication literature, Levine and McCornack (1991, p. 328) suggest that suspicion leads individuals to "more actively process" incoming information. In DeCarlo's (2005) marketing study, he suggests that suspicion increases "sophisticated attributional thought processes" (p. 239). And, in the Lyons et al. (2010) study on information technology, it is suggested that suspicion is associated with increased cognition (e.g., more information search tactics).

In summary, the construct of suspicion involves uncertainty about someone's (or something's) behavior. This uncertainty is also related to attributions of possible intent – and often malintent, concerns about being harmed, etc. Being in a state of suspicion also involves increased cognitive activity and load, because the actor (the suspicious person) is actively engaged in collecting data about another's motives or cognitively generating alternative explanations for the observed behavior (cf. Campbell & Kirmani, 2000; DeCarlo, 2005; Fein, 1996; Levine & McCornack, 1991; Lyons et al., 2011). Also, as suggested above, none of these components by themselves are sufficient for generating increased (or reduced) states of suspicion.

[2] We also note that in positive instances involving suspicion, the uncertainty is enjoyable (e.g., party giving; what song a dj is going to play next). Indeed, in management contexts, entrepreneurs might enjoy the uncertainty and risk associated with business ventures, as well as attempts to unpack suspicions about their competitors (cf. LeFevre, Matheny, & Kolt, 2003, who discuss occupational stress and the concept of positive stress, or eustress). However, the negative instances associated with suspicion (e.g., "I suspect that person might be trying to do me harm and might be acting intentionally deviously"; "I am suspicious of the information being given me by the automated read-out") are more fundamentally related to the cyber focus of this review.

For example, one can be uncertain, yet not suspicious, about tomorrow's weather; conversely, as noted by a reviewer, one can be certain that an external agent is an enemy and has strong malintent, yet still be suspicious of any observed behavior on that agent's part. Thus, it is the simultaneous combination of uncertainty, perceived (mal)intent, and cognitive activity (searching for alternative explanations or new data) that define state suspicion.[3]

3.5 State Suspicion in Information Technology (IT) Contexts

IT contexts might involve electronic *input*/collection of data (e.g., cataloging consumer purchases; determining the length of response time on a computer display) or automated *throughput*/analysis of such data (e.g., encoding, summarization, or interpretation via computer algorithms). IT contexts might also involve *output* such as decision making (e.g., offering alternative solutions to potential aircraft conflicts; generating potential preferences/rankings of possible troop movements) or electronic implementation of courses of action (e.g., generating automatic replies to customer queries). This summary is similar to the four purposes of automation noted by Lee and See (2004, citing Parasuraman et al., 2000); i.e., information acquisition, information analysis, decision selection, and action implementation. Thus, we define state suspicion in IT contexts as:

State suspicion in IT contexts is a person's simultaneous state of cognitive activity, uncertainty, and perceived malintent about underlying information that is being electronically generated, collated, sent, analyzed, or implemented by an external agent.

The "external agent" in this definition could be another person, a collection of individuals (e.g., a business organization or political group), or an inanimate object (e.g., a computer or an information system). For example, in our reading of the trust and automation literature, the concept of agent sometimes referred to (i) the operator of the IT system, (ii) the programmer/designer of the IT system, (iii) the programmer/developer of the algorithms used in the software, (iv) the software itself (without reference to the programmer, as in Bisantz & Seong, 2001), (v) the hardware in the system, (vi) the entire IT system (or perhaps linked mini-systems as in Buhler & Huhns, 2001), or (vii) the organization that is using the system (cf. Bobko, 2012). In our model, we suggest that an individual might have state suspicion about any of these agents.

3.6 Towards a Process-Based Model of Suspicion

In the application of trust to IT, Gefen, Benbasat, and Pavlou (2008) have noted a need for a conceptual framework to guide research. Thus, with our focus on IT suspicion, we also develop a three-stage process model of state-level IT suspicion.

As noted, there is a dearth of literature directly related to the definition, causes, and consequence of suspicion in IT contexts. The field is ripe for future research, and based on our review, analysis, and model (graphically depicted in Figure 1), we offer some formal propositions. We offer "research propositions" when the underlying theory appears sufficient to suggest a direction of effect for the underlying variables, as well as "exploratory research questions" when the literature is less well-specified.

[3] In statistical terminology, this definition implies a three-way interaction between cognitive activity, uncertainty, and malintent.

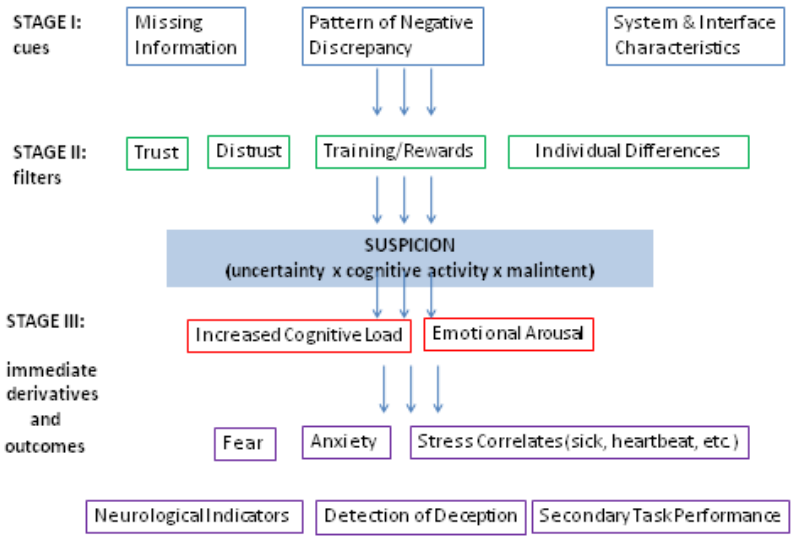

Figure 1: Stages of State-Level IT Suspicion

3.7 Suspicion Stage I: Cues in the IT Environment

Cues in the environment can act as a "trigger" of state-level suspicion (over and above baseline levels of trait suspicion, or tendency to be suspicious, noted in stage II). The Stage I cues include:

- *pattern of negative discrepancies*
- *missing information*
- *system and interface characteristics*

To generate relatively more specific cues, we used literature on decision making and missing information, as well as neurological literature. We also borrowed from the trust in automation literature because (i) there is currently minimal literature on IT suspicion and (ii) the trust in automation literature sometimes parallels our analysis of the general suspicion literature. For example, many trust in automation articles, almost by definition, assume that the external agent does not have to be an individual, but could, in fact, be an automated system or other

Second, articles in the trust in automation literature implicitly note the role of uncertainty (although the focus is uncertainty reduction) in their models (Jarvenpaa & Leidner, 1999; Lee & See, 2004; Lyons et al., 2011; McKnight, Choudhury, & Kacmar, 2002; Xu et al., 2007). Third, Lee and See (2004, p. 76) note that trust applies in automated situations -- where uncertainty and complexity make an exhaustive evaluation of options impractical. This relates to our notion that suspicion involves a generation of alternatives.

In summary, Table 2 delineates and categorizes factors which likely apply as Stage I cues to our state-level suspicion process. Based on finding in the literature, we expanded the missing information category to include incomplete or clarifying information; the discrepancy category was also enhanced, to include reliability and validity. Associated research citations are provided.

Table 2: Possible Input Factors at Stage 1 of the State Suspicion Process
(based on Figure 1)

MISSING, INCOMPLETE, OR CLARIFYING INFORMATION
Capacity to observe performance of the system (Lee & See, 2004)
Explanation/understandability of the algorithms and operations and their intent; clarity of benefit of automation (Lee & See, 2004; Lyons et al., 2011; Merritt & Ilgen, 2008, citing Muir, 1994; Parasuraman & Riley, 1997)
Specificity of system information (e.g., information support or specific recommendation; see Parasuraman & Manzey's, 2010, review p. 396 or Metzger et al., 2010)
Information perceived as missing (Ebenbach & Moore, 2000).
Structural assurances (e.g., on a web site or system confidence information) (McKnight et al., 2002; Parasuraman & Manzey, 2010, although not supported in Wang & Benbasat, 2008) and branding alliances (Lowry et al., 2008)
Willingness of persons in an electronic social system to provide personal information (Ridings, Gefen, & Arinze, 2002)
Whether the information is focused on positive feedback (all systems working) or focused on negatives (warnings); Lee and See (2004) note individuals are more cautious in the latter condition
PATTERN OF NEGATIVE DISCREPANCIES, RELIABILITY, AND VALIDITY
The patterns across time of failures in the system (Bisantz & Seong, 2001); for example, framing effects due to initial expectations (Lee & See, 2004)
Normality of the organizational structure and/or technical situation, or assurances thereof (Li et al., 2008)
Reliability and predictability of software being used (Jarvenpaa & Leidner, 1999, for predictable communication; Lee & See, 2004; Lyons et al., 2011; Parasuraman & Riley, 1997)
Reliability of hardware being used (Bailey & Scerbo, 2007, citing Lee & Moray, 1992; Merritt & Ilgen, 2008)
Integrity of the software's algorithms (matching to values of the user, Huhns & Buell, 2002; see also Lee & See's, 2004, notion of "value congruence")
Reputation of the system or vendor (Li et al., 2008; McKnight et al., 2002)
Accountability of the operator (cf. Parasuraman & Manzey's, 2010, discussion of work by Mosier and colleagues)
Accuracy or competence of the software being used (Huhns & Buell, 2002; Lyons et al., 2011; Merritt & Ilgen, 2008, citing Lee & Moray, 1992; Parasuraman & Riley, 1997)

Table 2: Possible Input Factors at Stage 1 of the State Suspicion Process (Continued)

ENVIRONMENTAL CUES VIA USER INTERFACE
Correspondence of visual interface with the actual environment being simulated (Bisantz & Seong, 2001)
Whether or not the interface is audiovisual, audio only, or text only (Burgoon, Blair, & Strom, 2005); it was found that truth bias was strongest in the audiovisual condition, but type of interface did not influence the accuracy of deception detection
Use of instant messaging in a running history, static format or just the current communication in a real-time format (Zhou & Zhang, 2007)
Etiquette (e.g., patience versus interruption) and politeness of any voice used (Parasuraman & Miller, 2004)
Timing of responses (Jarvenpaa & Leidner, 1999; Lee & See, 2004; Ridings, Gefen, & Arinze, 2002)
Use of real pictures, good colors, and provision of a physical address when web sites are being used (Lee & See, 2004)
Ease of use of a web site ("site quality" in McKnight et al., 2002; navigability, spelling, grammar in Metzger et al., 2010)
Use of instructive tone of voice versus informational tone (Cramer et al., 2008); the instructive agent was perceived as more competent although this was moderated by user locus of control
Matching of the emotion of any system voice with emotion of the user (Nass et al., 2005)
MISCELLANY
Time constraints (Parasuraman & Riley, 1997)
Task complexity (Parasuraman & Riley, 1997; Bailey & Scerbo, 2007)

For example, regarding discrepancies as cues, and consistent with the "uncertainty" component, state-level suspicion might be increased because of a mismatch between what is being perceived and what one expects. When operating a normally fast computer, a slow session might lead to a perceived discrepancy in expected speed, as well as generation of subsequent explanations (not enough RAM; malware; being monitored, etc.). Indeed, Oliveira, McDonald, and Goodman's (2007) neurological study supports this notion. They suggest that any discrepancies (positive or negative) between observation and expectation will be associated with increased anterior cingulate cortex activity – an indicator of increased need for cognition and use of external information.

Missing information is another possible environmental cue (via uncertainty and malintent) that increases state suspicion. In their marketing study, Johnson and Levin (1985) note that missing information is related to a reduction in predicted satisfaction (hence concern) with the potential purchase of a television. They note that missing information is particularly salient when the missing attribute is negatively correlated with other attributes. Indeed, these authors suggest that missing information induces "suspicion" (undefined). Other social science literature also supports the idea that missing information causes a devaluation of, or concern about, the focal object (e.g., Ebenbach & Moore, 2000, regarding environmental decisions about waste facility sites; Jagacinski, 1991, regarding personnel selection of hypothetical job candidates).

As an example of system and interface cues (our third category of Stage I variables), we note that the correspondence of actual and simulated environments, as well as ease of use of software, may reduce IT-induced suspicion (Bisantz & Seong, 2001; McKnight et al, 2002). Conversely, audio-only or text-only interfaces may increase suspicion relative to audiovisual interfaces (Burgoon et al., 2005).

The entries in Table 2, and our model in Figure 1, lead to our first two sets of "research propositions" for Stage I:

- Proposition I.1: A *pattern of negative discrepancies* between observed behavior by an external agent and predicted behavior of that agent will increase the observer's (user's) state-level suspicion. It may also be that a *single* discrepancy will have the same effect if the discrepancy is sufficiently large and harmful. In addition, *missing information* (external systems not responding completely; visual or audio input is impaired; etc.) will increase the user's level of state suspicion.
- Proposition I.2: Regarding cues and the *characteristics of IT system or situational attributes*, state-level IT suspicion will decrease (1) when there is a good correspondence between the visual interface and the actual environment being simulated, (2) when there is a capacity to observe performance of the system (either in terms of reliability or accuracy), (3a) when structural assurances about the system integrity and purpose are provided or (3b) when there is an explanation about the system's capabilities or purpose, (4) when system feedback is focused on systems working normally rather than feedback about potential negative events, (5) when system etiquette or politeness is high, (6) when responses are timely, (7) when system-based decisions are presented in a clear manner, (8) when the task is complex (in that complexity reduces monitoring), and (9) when the user generally perceives that the surrounding organization structure is normal. (See Table 2 for specific citations, supporting

studies, and other possible influential cues.) Conversely, levels of state-level IT suspicion will increase as the above factors become less prevalent or otherwise violate user expectations about the IT system.

We also suggest that Stage I determinants of state-level IT suspicion may be bypassed (directly to Stage III) by simply telling individual users to "be suspicious." We consider this possibility in the discussion section, when we note the need for research on the development of training programs.

A few "exploratory research questions" (offered when the literature is not as well- specified) about Stage I can also be generated. We hope they motivate future research, as well:

- Exploratory research questions I.1 (multivariate modeling): Mathematical models of the simultaneous operation of the multiple factors in Table 2 should be investigated. For example, consider two system precursors of suspicion from the above listings, i.e., explanation of system purpose (X_1) and physical representation of the simulated environment (X_2). If X_1 and X_2 are both positive, then presumably state suspicion is reduced. However, suppose X_1 is positive but X_2 is negative. Do these factors "cancel out" in the prediction of suspicion (i.e., an additive model)? Or, if either one of the variables is negative, will state suspicion be induced (i.e., an interactive model where if any variable is negative, this overrides all positive factors)? And, if the cues are all related to suspicion in the same direction, which cues are more salient (more heavily weighted) than others? To increase the interactive complexity, perhaps these models vary as a function of the individual difference moderators (catalysts and inhibitors) in Stage II.
- Exploratory research questions I.2a (negative events and framing): Research should consider how user behaviors are influenced by the pattern of previous successes and failures when interacting with specific IT systems. This notion might involve an application of the literature on cognitive heuristics (e.g., framing and anchoring) in human decision making (Metzger et al., 2010; Tversky & Kahneman, 1981). Such factors occasionally appear in the trust in automation literature (e.g., Lee & See, 2004 for framing). For example, although the two statements are arithmetically equivalent, does informing a user that a system works 95% of the time have different effects than informing a user that the system fails 5% of the time? Intuitively, the latter frame (perhaps any negative frame about reliability and accuracy) may induce more suspicion. Conversely, an argument could be made for the opposite effect; i.e., perhaps knowing that failure is occasionally a possibility may lead to less suspicion of the system because failure is a familiar outcome.[4]

[4] This latter possibility is analogous to classic reinforcement theory and the notion that behavior is more difficult to extinguish after variable ratio reinforcement (Reynolds, 1968). That is, under variable ratio reinforcement, one learns that an event (in this case a failure/event) occasionally occurs, so behavior (attitude toward the system) does not extinguish even when the data indicate otherwise.

- Exploratory research question I.2b (negative events and their magnitude): Research should also consider how the salience/importance of any failure influences the above processes. For example, if the failures that occur 5% of the time are each "small losses," is suspicion reduced due to "minor" failures being familiar? Conversely, there might be some threshold of failure importance, beyond which suspicion is aroused, regardless of prior experiences. We expect levels of this threshold to be correlated with individual differences as presented in Stage II. For example, an experienced computer user might quickly notice, and become suspicious about, a negative event, while a novice computer user might more readily blame him or herself in the presence of IT system failures, even if the system failures are substantial.
- Exploratory research questions I.3 (subliminal cues). We encourage research on the subliminal manipulation of cues listed in Table 2. For example, if a user is in a high state of suspicion, will subliminal messages on the user's screen (e.g., a subliminal display of the phrase "all is well") override any self-reported suspicion or physiological/neurological measures? Will behaviors focused on deception detection be reduced? There is support in the general literature for the influence of subliminal messages (cf. Mlodinow, 2012 for a review). For example, MacCrea et al. (1994) found that subjects' use of stereotyping could be manipulated subliminally. To the extent use of stereotypes is related to reduced cognitive energy, increased cognitive "misering", etc., it can be hypothesized that state suspicion could be reduced subliminally. Conversely, it might be possible to increase a user's cognitive activity and suspicion subliminally.

3.8 Suspicion Stage II: Individual Difference Determinants (Filters, Inhibitors, and Catalysts)

Individual differences might also play a major role in increasing, or inhibiting, state-level suspicion (e.g., trait level propensity to be suspicious or generalized distrust may act as catalysts). We discuss the following variables in our analysis and research propositions:

- *A user's trust in automation,* which decreases the likelihood of suspicion (via cognitive miser process)
- *A user's lack of trust (or distrust) in automation,* which increases the potential for suspicion
- *Other, correlated individual difference characteristics of the IT user,* such as faith in humanity, fatigue, overall tendency to trust, or self-efficacy
- *Training/rewarding* the user to embrace uncertainty and "be suspicious"

We first discuss the literature on trust and distrust, and then consider other individual differences variables that are likely to influence state-level suspicion in IT contexts.

The role of trust and distrust; related but conceptually distinct concepts**.** The most cited article on the construct of interpersonal trust in the management literature is by Mayer, Davis, and Schoorman (1995). Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor irrespective of the ability to monitor or control that other party" (p. 712). Note that there is an *expectation* involved in the decision to trust someone; i.e., a substantial reduction in uncertainty (see also Wang & Benbasat, 2008). In another highly cited article

(McAllister, 1995), trust is also linked to reductions in uncertainty.[5] Indeed, Colquitt et al. (2012) empirically found that both of McAllister's sub-dimensions of trust were negatively correlated with uncertainty (-.47 and -.55, for affect-based and cognition-based trust, respectively).

From the above, we suggest that trust involves a decision to act; in contrast, state suspicion is a cognitive process based in part on uncertainty. If a decision has already been formed, uncertainty is reduced and thus suspicion is reduced. As such, predispositions to trust are predispositions that remove uncertainty. Thus, predispositions to trust will inhibit increases in state-level suspicion by de-emphasizing the perception or incorporation of cues from the IT context. The existing literature hints at the above hypothesis. For example, Lee and See (2004) and McKnight, Choudhury, and Kacmar (2002) imply that trust, because it reduces uncertainty, may reduce the likelihood of suspicion. Buller and Bugoon (1996) also imply that trust inhibits suspicion, but via a somewhat different perspective – i.e., trust leads to truth bias (a tendency to assume that someone is truthful, regardless of the veracity).

More specifically, if one sees inconsistent behavior from a trusted external agent, one is less likely to attribute malintent to that entity and is less likely to engage in cognitive effort that generates alternative explanations for observed behavior. That is, trust, like stereotypes, economizes cognition (cf. Gilbert & Hixon, 1991; MacCrae, Milne, & Bodenhausen, 1994; Sherman & Frost, 2000). Indeed, too much trust can lead to complacency (cf. Ray, Baker & Plowman, 2011, in management, or Bailey & Scerbo, 2007, and Parasuraman & Manzey, 2010, in the trust in automation literature).

Regarding distrust, there is some minimal literature which explicitly refers to "distrust" and the notion that distrust also involves a decision. For example, in social psychology, Sinaceur (2010) states that distrust is a "negative, unilateral *judgment*" (p. 544). Or, in management Lewicki, McAllister, and Bies (1998) define distrust as "*confident* [italics added for emphasis] negative expectations regarding another's conduct." Although distrust thus implies a decision (about intent), we propose that distrust can indeed be a catalyst for state-level suspicion -- by focusing one's cognitive activity on that agent's uncertain future behavior. Thus, given distrust, the emergence of suspicion is not focused on the (mal)intent of the external agent, but is focused on cognitive activity and uncertainty regarding the agent's unknown behavior (and possible safeguards against that behavior).

[5] Although the articles by Mayer and McAllister, and their focus on interpersonal trust, continue to dominate management and applied psychology, other researchers suggest that trust can occur at many levels and with many different types of agents (cf. Lee & See, 2004). That is, trust is also considered to occur within/between virtual teams or virtual communities (e.g., Jarvenpaa & Leidner, 1999; Ridings, Gefen, & Arinze, 2002), countries (e.g., Hoffman, 2007), internet websites (e.g., McKnight, Kacmar, & Choudhury, 2004), automated decision aids (e.g., Huhns & Buell, 2002; Lyons et al., 2011), and new technology (e.g., Li, Hess, & Valacich, 2008).

For completeness, we note that the ambivalent feeling of "neither trust nor distrust" could lead to both kinds of cognitive engagement associated with state-level suspicion – activity focused on uncertainty about the agent's motives and the agent's possible future actions. In sum, our Stage II propositions about the role of trust and distrust are:

- Proposition II.1: In the face of anomalies in the system, relatively high levels of user trust act as an inhibitor to increases in state suspicion. In contrast, distrust leads to cognitive engagement associated with suspicion, but only for cognitive activity regarding possible alternative future actions of the external agent, and not the direction of the (mal)intent. Further, individual users who neither trust nor distrust external agents will, in the face of anomalies, engage in both types of cognitive activity associated with state suspicion – cognitive activity focused on the agent's possible intent and cognitive activity focused on the agent's possible future actions.

Other individual difference antecedents of state-level suspicion**.** Given our definition of suspicion, we hypothesize several other individual difference variables (creativity, need for cognition, intelligence) that are likely to be empirically correlated with levels of state suspicion.

First, it is suggested that creative individuals will be better able to be suspicious. Griffin and Moorhead (2010) define creativity as the "ability to generate new ideas or to conceive of new perspectives on existing ideas" (p. 210), and tests of creativity even include the "alternative uses test" (see Lissitz & Willhoft, 1985). Thus, given that state suspicion involves generating alternative explanations, we suggest that the capacity to be suspicious is conceptually linked to individual levels of creativity.

Second, work by Echebarria-Echabe (2010) suggests that the "need for cognition" may increase levels of suspicion, because such individuals are "more willing to engage in systematic processing" (p. 156). For example, Cacioppo and Petty (1982) developed a need for cognition scale which includes items such as "I would prefer complex to simple problems." We hypothesize that the need for cognition will be positively related to increased levels of suspicion due to the cognitive activity component of suspicion. In contrast, individuals low on need for cognition may be motivated to take things at face value. Such a notion (related to the concept of "cognitive misers") appears in the social psychology (Priester & Petty, 1995) and human factors (cf. Parasuraman & Manzey, 2010, citing Wickens & Hollands, 2000) literatures.

Third, in regard to task performance in suspicious contexts (e.g., the detection of deception), we hypothesize that individuals who are high on measures of general intelligence (i.e., have higher cognitive capacity, "*g*") are more capable of performing in environments that require increased state suspicion. Given the above cognitive nature of suspicion (coding/acquisition of information in the context of uncertainty; generating alternative explanations) suspicious individuals are cognitively busy. As Vonk (1998) demonstrated, suspicious individuals process incoming information less quickly. In turn, high-*g* individuals will be better able (than low-*g* individuals) to detect deception and function on other tasks while engaging in suspicious thoughts.

As noted earlier, there was little mention of the construct of suspicion in the human factors literature (exceptions being Lyons et al., 2011, and Parasuraman & Riley, 1997).

However, we borrow from the extensive trust in automation literature to suggest yet other individual difference factors in Stage II of our model. That literature suggests:

- Experience and familiarity with the technology (Lee & See, 2004; Lyons et al., 2011; see also Potosky & Bobko, 1998, or Potosky, 2007 for scales that assess computing experience)
- Faith in humanity (Li et al., 2008)
- Tendency to take a trusting stance and general levels of trust (Li et al., 2008; Ridings, Gefen, & Arinze, 2002)
- Conformity, inclination to use stereotypes, general negative affect, and cynicism (Bobko, 2012; Gefen et al., 2008)
- Self-efficacy and competence ("user accuracy") (Parasuraman & Miller, 2004; Parasuraman & Riley, 1997)
- Cost-benefit calculation by the user (Li et al., 2008; Wang & Benbasat, 2008)
- Workload and fatigue (Parasuraman & Riley, 1997).

For example, to the extent that faith in humanity or self-efficacy regarding technology are positively related to trust propensity, then these factors are likely to influence suspicion at Stage II (see also Parasuraman & Riley, 1997). Other dispositions that might be associated with reduced state-level suspicion, all else equal, include conformity or tendency to use stereotypes (Bobko, 2012) or other personality traits (Gefen et al., 2008). Still other characteristics of the user might be more situation specific, and include perceptions of individual workload (Parasuraman & Riley, 1997) or familiarity with the particular technology (Lee & See, 2004). We offer the following propositions regarding Stage II in our model:

- Proposition II.2: *Individual differences across users* will influence levels of IT state- level suspicion. Specifically, levels of suspicion will be increased when the user (1) lacks familiarity with similar systems, (2) has had some unexpected negative experiences with similar systems, (3) lacks faith in humanity, (4) tends to take cynical stances, (5) lacks self-efficacy and perceived individual competence, (6) has a minimal routine workload, and (7) has a high need for cognition. Conversely, *inhibitors* to increased levels of IT state-level suspicion include (1) positive experiences and familiarity with similar systems, (2) faith in humanity, (3) tendency to take a trusting stance and general disposition to trust, (4) self-efficacy and perceived personal competence, and (5) high workload and/or fatigue.
- Proposition II.2a : *Individual differences across users* will also influence the detection of anomalies during suspicious conditions. Specifically, increased detection success will be associated with increased user (a) intelligence (i.e., general cognitive ability) and (b) creativity.
- Proposition II.3: The individual differences in Proposition II and the situational characteristics in Proposition I will combine in an interactive manner (cf. Bobko, 2001) to predict levels of state suspicion. For example, consider the individual difference variable of "experience with similar systems" and the situational characteristic of "correspondence between visual interface and simulated environment." The state-level suspicion of highly experienced operators (e.g., expert operators) will be increased by relatively small discrepancies between

interfaces and simulated environments. In contrast, inexperienced users will require larger discrepancies before their state-level suspicion is increased.

3.9 Suspicion Stage III: Immediate Derivatives and Outcomes

Our definition and analysis of state-level IT suspicion suggested that when one is in a suspicious state (Stage III), cognitive activity/load is increased. During this stage, the user's cognitive activity is a central (but, as noted, not sufficient) component of state-level suspicion. Such cognitive activity occurs because the suspicious observer is engaged in (1) looking for alternative "pieces" of information, as well as (2) generating alternative explanations for observed behavior. In an empirical confirmation of this increased cognitive processing, Vonk (1998) demonstrated that suspicious subjects took longer to read textual stimuli than less suspicious subjects (see also Buller & Burgoon, 1996). Conversely, Parasuraman and Manzey (2010, citing Weiner) note the link between complacency (and lower cognitive load) and a lack of suspicion. Indeed, recent neurologically based studies indicate that suspicion involves substantial cognition (cf. Dimoka, 2010).

We suggest that state suspicion at Stage III is also associated with emotional reactions – but they would be reactions of anxiety and fear (given the uncertainty component), whereas distrust might be associated with reactions of anger (about a negative event and its causal agent). We note these immediate outcomes in our model. Indeed, Huddy and Feldman's (2011) analysis of reactions to the events of 9/11/01 suggest that, in negative situations, anxiety was linked to uncertainty whereas anger was linked to certainty. In yet another context (political doves versus hawks), a similar suggestion was made in Mahoney's (2011) analysis of the Cuban missile crisis in the 1960s. Mahoney states that the hawk's view of the crisis was "predictable" and "controllable," whereas the dove's view of the crisis was, among other things, "unpredictable." The doves thus felt "enormous anxiety throughout, while the hawks felt virtually none" (p. 204). Our research propositions for immediate, psychological consequences of Stage III are:

- Proposition III.1: As individual users become more suspicious, their cognitive load will increase (and markers of cognitive load such as working memory or speed of processing will decrease). Further, as state suspicion increases, the (mal)intent and uncertainty facets will result in increased emotional arousal (characterized by fear and anxiety rather than by anger).

In regard to hypotheses about neurological indicators of state-level suspicion, Watabe, Ban, and Yamamoto (2011) note that it is difficult to identify specific decision-making processes based upon differential brain activation, given the interconnectedness of the influence of brain regions. Nonetheless, we draw some tentative research propositions about the identification and measurement of IT induced state-level suspicion.

It was noted earlier that one potential cause of state-level suspicion was a discrepancy between what one expects and what one observes. Such a discrepancy could lead to cognitive activity dedicated to searching for explanations of the discrepancy, causing increased uncertainty, decreased trust, etc. Oliveira, McDonald, and Goodman (2007) conducted two EEG studies based on the assumption that the anterior cingulated cortex (ACC) in the brain is involved in (i) error detection or (ii) evaluation of poor performance (cf. also Hajcak, McDonald, & Simmons, 2004). Note that error recognition and performance evaluation are two representations of increased cognitive activity. Further, Oliveira et al. found that ACC activity occurs for unexpected rewards, as well as increases in rewards. This converges with our "uncertainty"

facet of suspicion (whether positive or negative). Oliveira et al. also suggested that the ACC acts as a system which signals an increased need for cognitive control, an updating of one's internal models, and increased use of external information. These processes all directly reflect the increased active cognition facet of our definition of state-level suspicion. Thus, we suggest:

- Proposition III.2: Increased levels of IT suspicion will be associated with increased anterior cingulate cortex activity.

Regarding emotion and the neurological literature, Hajcak et al. (2004) found that if an individual's uncertainty was perceived to have potentially negative consequences (which reflects our focus on malintent in IT contexts), then anxiety would be increased due to the interaction of potential negativity and hyper-arousal (cognitive activity). This links with our suggestion that suspicion will be associated with increased anxiety (rather than, say, increased anger). However, one moderator to the above hypothesis might involve mood of the IT user. That is, Hajack et al. (2004) found that negative affect/mood increased error-related negativity (ERN), while reducing an error positivity (Pe) measure. In other words, participants who were relatively high in negative affectivity noticed errors more strongly, but they were also less likely to cognitively process those errors and/or update any mental models about what was happening.

Stickney (2009; citing Schwartz, 2000) also notes that mood influences decision making strategy; i.e., a sad mood leads to more attention to detail and less reliance on pre-existing strategies, whereas a positive mood is linked to greater use of heuristics. This implies that negative mood is more strongly related to suspicion than is positive mood, given the process of generating alternative explanations when suspicious. Thus, we suggest:

- Proposition III.3: Individuals who are experiencing a negative mood (due to long-term trait or shorter term situational reasons), will be more likely to become suspicious than positive mood individuals.

Going a step further, we note that other researchers (e.g., Marsland et al., 2006) state that negative affect is associated with right-sided prefrontal brain activity and positive affect is associated with left-sided prefrontal activity. Interestingly, this converges with recent work in the management literature (Waldman, Balthazard, & Peterson, 2011) on the link between neuroscience and "inspirational leadership." These authors note that right frontal brain dysfunction is associated with difficulties in dealing with uncertainty. Given that uncertainty is a facet of suspicion, we might suggest that researchers also look for associations between right-sided prefrontal activity and increased levels of suspicion. However, another facet of suspicion is increased cognitive activity, which would increase activation in both sides of the brain. Hence we refrain from any specific propositions in this regard.

Further, researchers conducting "theory of mind" (ToM; Premack & Woodruff, 1978) studies have found that the anterior paracingulate cortex is activated when participants are deciding whether or not to cooperate with, or trust, someone else (e.g., Gallagher & Frith, 2003). That is, higher brain activation in the anterior paracingulate cortex has been associated with the cognitively demanding process by which a person infers whether or not another person is trustworthy. Such activation is consistent with the findings of Dimoka (2010), Gefen et al. (2008), and Kreuger et al. (2007). However, Dimoka additionally found that subjects who were given ambiguous information (i.e., subjects in the condition of no trusting information and no distrusting information) were also prone to increases in anterior paracingulate cortex activity.

We suggest this is because the ambiguous information could breed suspicion which, in turn, would also lead to increased cognitive activity. This more general link between cognitive activity and anterior paracingulate cortex activity (whether via a decision process about trust or due to informational ambiguity) is consistent with the theory of mind. Thus, we suggest:

- Proposition III.4: Increases in paracingulate cortex activity will be associated with (i) individuals in the process of making decisions about trust (or distrust) or (ii) individuals who are receiving ambiguous information. Conversely, decreases in paracingulate cortex activity will be associated with individuals who have made decisions about trust (or distrust), because these individuals invoke cognitive heuristics to quickly and efficiently process future information.

Regarding more distal outcomes, to the extent that state-level suspicion induces fear and anxiety, then suspicion will be associated with indicators of arousal, such as increased blood pressure and electrodermal activity (EDA). If the suspicion, and associated stress, is sustained across time then long-term outcomes might be increased susceptibility to colds or even increased likelihood of coronary heart disease (Friedman & Ulmer, 1984; Myers, 2010).

We also suggest that an increase in state-level suspicion will be associated with an increased ability to correctly detect deception. Consistent with our propositions about individual differences, it is further hypothesized that detection of deception is also enhanced by increased levels of individual cognitive ability and/or creativity (because these individual difference factors enhance one's capacity to generate alternative possibilities and be suspicious). Note also that the above suggestions assume that there is some deception to be detected. This leads to:

- Exploratory research question III.1 (warranted suspicion): Are there appropriate levels of suspicion, and what is the nature of the relationship between levels of suspicion and successful detection of deception? Presumably, such a relationship is curvilinear. That is, as suspicion increases, detection of suspicious events increases, but at a particular point generalized suspicion is unwarranted (Parasuraman & Riley, 1997, discuss the use, abuse, disuse, and misuse of automated systems and the phrase "unwarranted suspicion"). If some individuals are pre-disposed to be suspicious (see Table 2), then they are pre- disposed to spend cognitive energy generating alternative possibilities. Will this expenditure of cognitive resources then reduce their capacity to sometimes "see the obvious"?

3.10 Summary

One purpose of the current review was to conduct a multi-disciplinary review of the (minimal) research on suspicion – with a specific focus on IT induced, state-level suspicion. The few existing articles from each of several social science domains were considered, and inconsistencies/consistencies were noted. The integrative definition of suspicion has the key components of "uncertainty," "cognitive activity," and "(mal)intent." In particular, we defined IT state-level suspicion as a person's *simultaneous* state of cognitive activity, uncertainty and perceived malintent about underlying information that is being electronically generated, collated, sent, analyzed, or implemented by an external agent.

A three-stage, heuristic model of suspicion was developed, aided by other, related literatures regarding the concepts of trust (in general) and trust-in-automation (in particular). This led to several research propositions and exploratory questions about the concept of IT-induced, state-

level suspicion at each of the three stages. We believe that attention to a common definition of suspicion, and research on the above propositions/questions, will assist both academicians and practitioners who desire to embrace the notion of suspicion in technologically enhanced contexts.

Other efforts might readily follow beyond those listed in this review. For example, use of a theoretically-based, uniform definition of "state-level suspicion" by different social scientists could lead to a more reliable and valid measure of suspicion. Self-report items could be developed (particularly about the interactive facets of uncertainty, cognition, and intent), as well as physiological and neurological measures. To further assess construct validity, the self-report measures could be triangulated with neurological measures (paralleling Hancock et al.'s, 2011, call for assessments of measurement convergence in the human-robot interaction literature).

Measurement items might also be categorized as assessing the ability to be suspicious (e.g., capacity to generate alternative explanations; capacity to recognize relevant cues, capacity to accurately detect deception) or the motivation to be suspicious (i.e., attentiveness to cues across time). These two types of criteria match the usual "can do" and "will do" distinction in studies on job performance in management and applied psychology (Borman, White, Pulakos, & Oppler, 1991).

Given this uniformly accepted definition/measure of suspicion, the nomological net of correlates discussed earlier could be empirically investigated in order to further enhance the understanding of suspicion. Several possible correlates were noted in our discussion of Stage II (e.g., intelligence, creativity, need for cognition, disposition to trust, cynicism). As suggested by others (Bond & Lee, 2005; Levine & McCornack, 1991) it is also useful to distinguish between "trait" and "state" suspicion. That is, it may be that some individuals are predisposed to be suspicious (cf. the suggested correlate of "faith in humanity"). On the other hand, our focus has been on "suspicion" as a transient state that is dependent on IT-induced situational factors. For example, we noted a variety of system/machine characteristics that could influence levels of state suspicion. Benbasat, Gefen, and Pavlou (2008) noted a variety of moderators of user trust in IT systems, which might also apply to research on IT suspicion (e.g., moderators such as gender and culture). Indeed, one of the primary dimensions of globally-based culture is labeled "uncertainty avoidance" (Hofstede & Bond, 1988, p. 11), which involves relative discomfort in unstructured, unknown, or surprising situations. Thus, individuals from such cultures may be less likely to engage in suspicious behaviors, as they have a desire to avoid the "uncertainty" component in our definition of suspicion.

Further, if suspicion can indeed be influenced, and if suspicion is both an ability (can do) and attitude (will do), suspicion might be trained via programs involving attitude formation and training. Attitudes are considered to have three components – cognitive, affective, and behavioral intent (e.g., Griffin & Moorhead, 2010) – and the first two attitudinal components mirror the active cognition facet of suspicion and the arousal/anxiety outcomes discussed above.

"Suspicion training" might also be informed by the IT literature. For example, it has been suggested that operator performance is readily influenced/enhanced by requiring the operator to occasionally shift from automated to manual modes (e.g., Chen, Barnes, & Harper-Sciarini, 2010; Lee & See, 2004; Parasurman & Manzey, 2010, citing work by Gopher and work by Metzger). Therefore, the active cognition component of suspicion may be enhanced by having users occasionally switch modes (of information acquisition or responding) rather than succumb to complacency via continued use of a single channel. As another example, the US Army has

adopted a program, based on positive psychology, which builds soldier resilience by training those individuals to avoid worst-scenario thinking (see Cornum, Matthews, & Seligman, 2011, for an overview of this program). It is interesting to speculate whether or not suspicion training (particularly raising cognitive awareness and motivation to consider the possibility of malintent) might be counter to such a program.

In addition, the focus of the current review has been on the "receiver"; i.e., the focus has been on the person who might be suspicious, what that person's characteristics might be, and how that person might react to, or process information from, situational cues, etc. A different set of research activities might focus on behaviors and attributes of the person/entity who is attempting the deception. We imagine several parallel processes; e.g., increased cognitive load for the "deceiver" (external agent). For example, in the law enforcement literature, a variety of studies indicates that being deceptive is more cognitively demanding than being truthful (for a review, see Patterson, 2009, who also notes that behavioral indicators of increased load include reduced eye blinks and reduced excess body movement). Or, in applied psychology, both Ziegler (2011) and van Hooft and Born (2012) used eye-tracking measures to assess the cognitive load of individuals who were trying to fake on self-report personality tests.

Finally, as noted in one of our research questions, research on the use of subliminal information might be particularly promising. Such research has existed for decades in marketing, but seems to be readily linked to IT contexts (e.g., individuals working at computer displays).

For example, we noted that MacCrae et al. (1994) found that stereotypes could be subliminally induced, and such stereotypes were associated with cognitive relaxation (in contrast to increased cognitive activity). It would be interesting to see if state suspicion could be subliminally induced or reduced (and what ways were most effective in doing so). For example, experiments could be conducted that subliminally manipulated factors such as perceptions of fatigue, system accuracy, history of prior distrusting experiences, etc. in order to see influences on suspicion.

In summary, the potential for research on suspicion, and IT state suspicion, is vast and has important implications. We hope the integrative review, definition, process, and propositions assist future researchers in this domain. We look forward to the results that such research will bring.

3.11 Key Points

- There is little in the human factors literature on the important topic of suspicion.
- We develop a definition and integrative model of IT induced, state-level suspicion based upon work in communication, psychology, human factors, management, marketing, information technology, and neuropsychology.
- The definition of state suspicion is the simultaneous occurrence of (a) uncertainty, (b) increased cognitive processing (e.g., generation of alternative explanations for perceived discrepancies), and (c) perceptions of malintent.
- Research propositions within IT contexts are derived at each of three stages in our model of suspicion.

4.0 REFERENCES

Bailey, N., & Scerbo, M. (2007). Automation-Induced Complacency for Monitoring Highly Reliable Systems: The Role of Task Complexity, System Experience, and Operator Trust. *Theoretical Issues in Ergonomics Science, 8,* 321-348.

Benbasat, I, Gefen, D., &Pavlou, P. (2008). Special Issue: Trust in Online Environments. *Journal of Management Information Systems, 24,* 5-11.

Bisantz, A., & Seong, Y. (2001). Assessment of Operator Trust in Utilization of Automated Decision-Aids under Different Framing Conditions. *International Journal of Industrial Ergonomic, 28,* 85-97.

Bobko, P. (2001). *Correlation and Regression (rev. ed.).* Thousand Oaks, CA: Sage Press.

Bobko, P. (2012). *A Review and Analysis Of Suspicion (and IT Suspicion) as a Psychological Construct: Interim report.* Air Force Research Laboratory, 711th Human Performance Wing, ICER Contract No FA8650-09-D-6939, Dayton, OH: Wright Patterson AFR, OH

Bond, G. (2012). Focus on Basic Cognitive Mechanisms and Strategies in Deception Research (and Remand Custody of 'Wizards' to Harry Potter movies). *Journal of Applied Research in Memory and Cognition, 1,* 128-130.

Bond, G., & Lee, A. (2005). The Darkest Side of Trust: Validating the Generalized Communication Suspicion Scale with Prison Inmates. *Personality and Individual Differences, 38,* 1429-1438.

Borman, W., White, L., Pulakos, E., & Oppler, S. (1991). Models of Supervisor Kob Performance Ratings. *Journal of Applied Psychology, 76,* 863-872.

Buhler, P., & Huhns, M. (2001). Trust and Persistence. *IEEE Internet Computing, 5,* 85-87.
Buller, D., & Burgoon, J. (1996). Interpersonal Deception Theory. *Communication Theory, 3,* 203-242.

Burgoon, J., Blair, J., & Strom, R. (2005). Heuristics and Modalities in Determining Truth versus Deception. *Proceedings of the 38th Hawaii International Conference on System Sciences,* 1-8.

Buss, A., & Durkee, A. (1957). An Inventory for Assessing Different Kinds of Hostility. *Journal of Consulting Psychology, 21,* 343-349.

Buss, A., & Perry, M. (1992). The Aggression Questionnaire. *Journal of Personality and Social Psychology, 63,* 452-459.

Cacioppo, J., & Petty, R. (1982). The Need for Cognition. *Journal of Personality and Social Psychology, 42,* 116-131.

Campbell, M., & Kirmani, A. (2000). Consumer's Use of Persuasion Knowledge: The Effects of Accessibility and Cognitive Capacity on Perceptions of an Influence Agent. *Journal of Consumer Research, 27,* 69-83.

Chen, J., Barnes, M., & Harper-Sciarini, M. (2010). Supervisory Control of Multiple Robots: Human-Performance Issues and User-Interface Design. *IEEE Transactions on Systems, Man, and Cybernetics – Part C, Applications and Reviews, 41,* 435-454.

Colquitt, J., LePine, J., Piccolo, R., Zapata, C., & Rich, B. (2012). Explaining the Justice-Performance Relationship: Trust as Exchange Deepener or Trust as Uncertainty Reducer. *Journal of Applied Psychology, 97,* 1-15.

Cornum, R., Matthews, M., & Seligman, M. (2011). Comprehensive Soldier Fitness: Building Resilience in a Challenging Institutional Context. *American Psychologist, 66,* 4-9.

Cramer, H., Evers, V., Kemper, N., & Wielinga, B. (2008). Effects of Autonomy, Traffic Conditions and Driver Personality Traits on Attitudes and Trust Towards In-Vehicle Agents. *IEEE International Conference on Web Intelligence and Intelligent Agent Technology*, 477-482.

DeCarlo, T. (2005). The Effects of Sales Message and Suspicion of Ulterior Motives on Sales Person Evaluation. *Journal of Consumer Psychology, 15,* 238-249.

Deutsch, M. (1958). Trust and Suspicion. *The Journal of Conflict Resolution, 2,* 265-279.
Dimoka, A. (2010). What does the Brain Tell us about Trust and Distrust? Evidence from a Functional Neuroimaging Study. *MIS Quarterly, 34,* 1-24.

Ebenbach, D., & Moore, C. (2000). Incomplete Information, Inferences, and Individual Differences: The Case of Environmental Judgments. *Organizational Behavior and Human Decision Processes, 81,* 1-27.

Echebarria-Echabe, A. (2010). Effects of Suspicion on Willingness to Engage in Systematic Processing of Persuasive Arguments. *The Journal of Social Psychology, 150,* 148-159.

Fein, S. (1996). Effects of Suspicion on Attributional Thinking and the Correspondence Bias. *Journal of Personality and Social Psychology, 70,* 1164-1184.

Ferrin, D., & Dirks, K. (2003). The Use of Rewards to Increase and Decrease Trust: Mediating Processes and Differential Effects. *Organization Science, 14,* 18-31.

Friedman, M. & Ulmer, D. (1984). *Treating Type-A Behavior and your Heart*. New York, NY: Knopf.

Gallagher, H., & Frith, C. (2003). Functional Imaging of "Theory of Mind." *Trends in Cognitive Science, 7,* 77-83.

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A Research Agenda for Trust in Online Experiments. *Journal of Management Information Systems, 24,* 275-286.

Gilbert, D., & Hixon, G. (1991). The Trouble of Thinking: Activation and Application of Stereotypic Beliefs. *Journal of Personality and Social Psychology, 60,* 509-517.

Grant, A., & Hofmann, D. (2011). Outsourcing Inspiration: The Performance Effects of Ideological Messages from Leaders and Beneficiaries. *Organizational Behavior and Human Decision Processes, 116,* 173-187.

Griffin, R., & Moorhead, G. (2010). *Organizational Behavior: Managing People and Organizations* (9th Ed.). Boston: Houghton Mifflin.

Hajcak, G., McDonald, N., & Simons, R. (2004). Error-Related Psychophysiology and Negative Affect. *Brain and Cognition, 56,* 189-197.

Hancock, P., Billings, D., Schaefer, K., Chen, J., de Visser, E., & Parasuraman, R. (2011). A Meta-Analysis of Factors Affecting Trust in Human-Robot Interaction. *Human Factors, 53,*

517-527.

Hilton, J., Fein, S., & Miller, D. (1993). Suspicion and Dispositional Inference. *Personality and Social Psychology Bulletin, 19*, 501-512.

Hoffman, A. (2007). The Structural Causes of Trusting Relationships: Why Rivals do not Overcome Suspicion Step-by-Step. *Political Science Quarterly, 122*, 287-312.

Hofstede, G., & Bond, M. (1988). The Confucious Connection: From Cultural Roots to Economic Growth. *Organizational Dynamics, 16*, 5-21.

Huddy, L., & Feldman, S. (2011). Americans Respond Politically to 9/11: Understanding the Impact of the Terrorist Acts and their Aftermath. *American Psychologist, 66*, 455-467.

Huhns, M., & Buell, D. (2002). Trusted Autonomy. *IEEE Internet Computing, 6*, 92-95.

Jagacinski, C. (1991). Personnel Decision Making: The Impact of Missing Information. *Journal of Applied Psychology, 76*, 19-30.

Jarvenpaa, S., & Leidner, D. (1999). Communication and Trust in Global Virtual Teams. *Organization Science, 10*, 791-815.

Johnson, R., & Levin, I. (1985). More than Meets the Eye: The Effect of Missing Information on Purchase Evaluations. *Journal of Consumer Research, 12*, 169-177.

Krueger, F., McCabe, K., Moll, J., Kriegeskorte, N., Zahn, R., Strenziok, M., Heinecke, A., & Grafman, J. (2007). Neural Correlates of Trust. *Proceedings of the National Academy of Sciences, 104*, 20084-20089.

Lee, J., & See K. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors, 46*, 50-80.

LeFevre, M., Matheny, J., & Kolt, G. (2003). Eustress, Distress, and Interpretation in Occupational Stress. *Journal of Managerial Psychology, 18*, 726-744.

Levine, T., & McCornack, S. (1991). The Dark Side of Trust: Conceptualizing and Measuring Types of Communicative Suspicion. *Communication Quarterly, 39*, 325- 340.

Lewicki, R., McAllister, D., & Bies, R. (1998). Trust and Distrust: New Relationships and Realities. *Academy of Management Review, 23*, 438-458.

Li, X., Hess, T., & Valacich, J. (2008). Why do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. *Journal of Strategic Information Systems, 17*, 39-71.

Lissitz, R., & Willhoft, J. (1985). A Methodological Study of the Torrance Tests of Creativity, *Journal of Educational Measurement, 22*, 1-11.

Lowry, P., Vance, A., Moody, G., Beckman, B., & Read, A. (2008). Explaining and Predicting the Impact of Branding Alliances and Web Site Quality on Initial Consumer Trust of e-Commerce Web Sites. *Journal of Management Information Systems, 24*, 199-224.

Lyons, J., Stokes, C., Eschleman, K., Alarcon, G., & Barelka, A. (2011). Trustworthiness and IT Suspicion: An Evaluation of the Nomological Network. *Human Factors*. Article Published Online 13 May 2011. DOI:10.1177/0018720811406726.

Maccrae, C., Milne, A., & Bodenhausen, G. (1994). Stereotypes as Energy-Saving Devices: A

Peek Inside the Cognitive Toolbox. *Journal of Personality and Social Psychology, 66,* 37-47.

Mahoney, R. (2011). *The Kennedy Brothers: The Rise and Fall of Jack and Bobby*. New York, NY: Arcade Publishing.

Marsland, A., Cohen, S., Rabin, B., & Manuck, S. (2006). Trait Positive Affect and Antibody Response to Hepatitis B Vaccination. *Brain, Behavior, and Immunity, 20,* 261-269.

Mayer, R., Davis, J., & Schoorman, D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20,* 709-734.

McAllister, D. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal, 38,* 24-59.

McKnight, D., Choudhury, V., & Kacmar, C. (2002). The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model. *Journal of Strategic Information Systems, 11,* 297-323.

McKnight, D., Kacmar, C., & Choudhury, V. (2004). Dispositional Trust and Distrust Distinctions in Predicting High- and Low-Risk Internet Expert Advice Site Perceptions. *e-Service Journal, 3,* 35-55.

Metzger, M., Flanagin, A., & Medders, R. (2010). Social and Heuristic Approaches to Credibility Evaluation Online. *Journal of Communication, 60,* 413-439.

Merritt, S., & Ilgen, D. (2008). Not all Trust is Created Equal: Dispositional and History-Based Trust in Human-Automation Interactions, *Human Factors, 50,* 194-210.

Mlodinow, L. (2012). *Subliminal: How your Unconscious Mind Rules your Behavior*. New York, NY: Vintage Books.

Myers, D. (2010). *Psychology (Ninth Ed.).* New York, NY: Worth Publishers.

Nass, C., Josson, I., Harris, H., Reaves, B., Endo, J., Brave, S., & Takayama, L. (2005). Improving Automotive Safety by Paring Driver Emotion and Car Voice Emotion. *Proceedings of the Human Factors in Computing Systems Conference, CHI,* 1973-1976.

Oliveira, F., McDonald, J., & Goodman, D. (2007). Performance Monitoring in the Anterior Cingulate is not all Error-Related: Expectancy Deviation and the Representation of Action-Outcome Associations. *Journal of Cognitive Neuroscience, 19,* 1994-2004.

Olson, N. (2009). *The Development of IT Suspicion as a Construct and Subsequent Measure*. Master's Thesis, Air Force Institute of Technology, Wright Patterson AFB, OH.

Parasuraman, R., & Manzey, D. (2010). Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors, 52,* 381-410.

Parasuraman, R., & Miller, C. (2004). Trust and Etiquette in High-Criticality Automated Systems. *Communication of the ACH, 4,* 51-55.

Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors, 39,* 230-253.

Patterson, T. (2009). *The Effect of Cognitive Load on Deception*. Unpublished Doctoral Dissertation, Florida International University, Miami, FL.

Potosky, D. (2007). The Internet Knowledge (iKnow) Measure, *Computers in Human Behavior,*

23, 2760-2777.

Potosky, D. & Bobko, P. (1998). The Computer Understanding and Experience Scale: A Self Report Measure of Computer Experience, *Computers in Human Behavior, 14*, 337-348

Premack, D., & Woodruff, G. (1978). Does the Chimpanzee have a Theory of Mind? *Behavioral Brain Science, 1*, 515-526.

Priester, J., & Petty, R. (1995). Source Attribution and Persuasion: Perceived Honesty as a Determinant of Message Scrutiny. *Personality and Social Psychology Bulletin, 21*, 637-654.

Ray, J., Baker, L., & Plowman, D. (2011). Organizational Mindfulness in Business Schools. *Academy of Management Learning and Education, 10*, 188-203.

Reynolds, G. (1968). A Primer of Operant Conditioning. New York: Scott, Foresman, and Company.

Ridings, C., Gefen, D. & Arinze, B. (2002). Some Antecedents and Effects of Trust in Virtual Communities. *Journal of Strategic Information Systems, 11*, 271-295.

Sherman, J., & Frost, L. (2000). On the Encoding of Stereotype-Relevant Information under Cognitive Load. *Personality and Social Psychology Bulletin, 26*, 26-34.

Sinaceur, M. (2010). Suspending Judgment to Create Value: Suspicion and Trust in Negotiation. *Journal of Experimental Social Psychology, 46*, 543-550.

Stickney, L. (2009). Affect and Decision Making. *Decision Line, May Issue*, 4-6.

Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science, 211*, 453-458.

van Hooft, E., & Born, M. (2012). Intentional Response Distortion on Personality Tests: Using Eye- Tracking to Understand Response Processes when Faking. *Journal of Applied Psychology,*

97, 301-316.

Vonk, R. (1998). The Slime Effect: Suspicion and Dislike of Likable Behavior towards Superiors. *Journal of Personality and Social Psychology, 74*, 849-864.

Waldman, D., Balthazard, P., & Peterson, S. (2011). Leadership and Neuroscience: Can we Revolutionize the Way that Inspirational Leaders are Identified and Developed? *Academy of Management Perspectives, February*, 60-74.

Wang, W., & Benbasat, I. (2008). Attributions of Trust in Decision Support Technologies: A Study of Recommendation Agents for e-Commerce. *Journal of Management Information Systems, 24*, 249-273.

Watabe, M., Ban, H., & Yamamoto, H. (2011). Judgments about Others' Trustworthiness: An fMRI study. *Letters on Evolutionary Behavioral Science, 2*, 28-32.

Xu, G., Feng, Z., Wu, H. & Zhao, D. (2007). Swift Trust in a Virtual Temporary System: A Model Based on the Dempster-Shafer Theory of Belief and Functions. *International Journal of Electronic Commerce, 12*, 93-126.

Yoon, Y., Gurhan-Canli, Z., & Schwarz, N. (2006). The Effect of Corporate Social Responsibility (CSR) Activities on Companies with Bad Reputations. *Journal of Consumer Psychology, 16*, 377-390.

Zhou, L., & Zhang, D. (2007). Typing or Messaging? Modality Effect on Deception Detection in Computer-Mediated Communication. *Decision Support Systems, 44*, 188-201.

Ziegler, M. (2011). Applicant Faking: A Look into the Black Box. *The Industrial-Organizational Psychologist, 49*, 29-36

LIST OF ACRONYMS

ACC	Anterior Cingulated Cortex
AFOSR	Air Force Office of Scientific Research
CA	Cognitive Activity
EDA	Electrodermal Activity
ERN	Error-Related Negativity
IT	Information Technology
MI	Mal-Intent
Pe	Error Positivity
Un	Uncertainty